

Digital Operational Resilience Act

Betroffenheit und notwendige Maßnahmen zur Compliance mit der EU-weiten Cybersicherheitsverordnung für den Finanzsektor

Mit dem Digital Operational Resilience Act (DORA) wird ein einheitlicher europäischer Rechtsrahmen für Cybersicherheitsanforderungen im Finanzsektor geschaffen. Ziel ist es, die operationelle Resilienz von Finanzunternehmen zu gewährleisten. Der DORA ist bereits in Kraft getreten und findet ab dem 17. Januar 2025 Anwendung.

Wer ist betroffen?

Der DORA richtet sich in erster Linie an Finanzunternehmen aus über 20 verschiedenen Branchen, darunter Kreditinstitute, Zahlungs- und Kontoinformationsdienstleister, Wertpapierfirmen, Versicherungs- und Rückversicherungsunternehmen sowie Einrichtungen der betrieblichen Altersversorgung. Darüber hinaus werden auch IKT-Drittdienstleister erfasst, die Finanzunternehmen mit IKT-Dienstleistungen unterstützen.

Was ist umzusetzen?

Die Anforderungen des DORA können in vier Hauptbereiche unterteilt werden. Der erste Bereich betrifft das IKT-Risikomanagement. Finanzunternehmen müssen einen internen Governance- und Kontrollrahmen einrichten, um IKT-Risiken effektiv zu identifizieren und darauf zu reagieren. Die Verantwortung für die Überwachung und Umsetzung liegt bei der Unternehmensleitung. Der zweite Bereich umfasst die Behandlung und Meldung von IKT-bezogenen Vorfällen. Unternehmen sind verpflichtet, ein Incident Management zu implementieren, das die Überwachung, Ursachenermittlung, Klassifizierung und Dokumentation von IKT-bezogenen Vorfällen umfasst. Der dritte Bereich betrifft Resilienztests. Die IKT-Resilienz muss regelmäßig durch umfassende Testverfahren wie Schwachstellenanalysen, Penetrationstests

und Netzwerksicherheitsbewertungen sichergestellt werden. Der vierte Bereich regelt schließlich das Management von Drittanbieterrisiken. Auch bei der Auslagerung an IKT-Drittdienstleister verbleibt die Verantwortung beim betroffenen Unternehmen. Es sind Risikoanalysen durchzuführen, ein Informationsregister zu führen und vertragliche Vereinbarungen mit vorgegebenen Mindestinhalten zu treffen. Für kleine Unternehmen gibt es teilweise Ausnahmen und Erleichterungen bei der Umsetzung einzelner Anforderungen.

Was droht bei Verstößen?

Aufsichtsbehörden wie die BaFin oder die EZB können Zwangsgelder verhängen, Weisungen erteilen und Verstöße öffentlich machen. Auch strafrechtliche Sanktionen sind möglich.

Unsere Unterstützung

Wir unterstützen Sie bei der Umsetzung der Anforderungen des DORA u.a. mit folgenden Leistungen:

- Rechtliche Prüfung der Betroffenheit Ihres Unternehmens
- Ableitung der konkreten Vorgaben für Ihr Unternehmen
- Rechtliche Unterstützung bei der Umsetzung und Dokumentation
- Einführung eines Cybersecurity Compliance Managements

Next Step: Kontaktaufnahme

Gerne erläutern wir Ihnen unser Vorgehen ausführlich in einem persönlichen Gespräch. Nehmen Sie jetzt unverbindlich Kontakt auf!

T + 49 30 / 2332 895 0

E info@reuschlaw.de